The Windows 2000 Public Key Infrastructure

Federal PKI TWG – February 1999

Brian A. LaMacchia
Program Manager, Core Cryptography

Agenda

- Windows 2000 PKI core components
- Client-side PKI components
  - Internet Explorer 5.0
- Server-side PKI components
  - Windows 2000 Certificates Services
- Enterprise-wide PKI features
  - Administration of enterprise-wide PKI policy

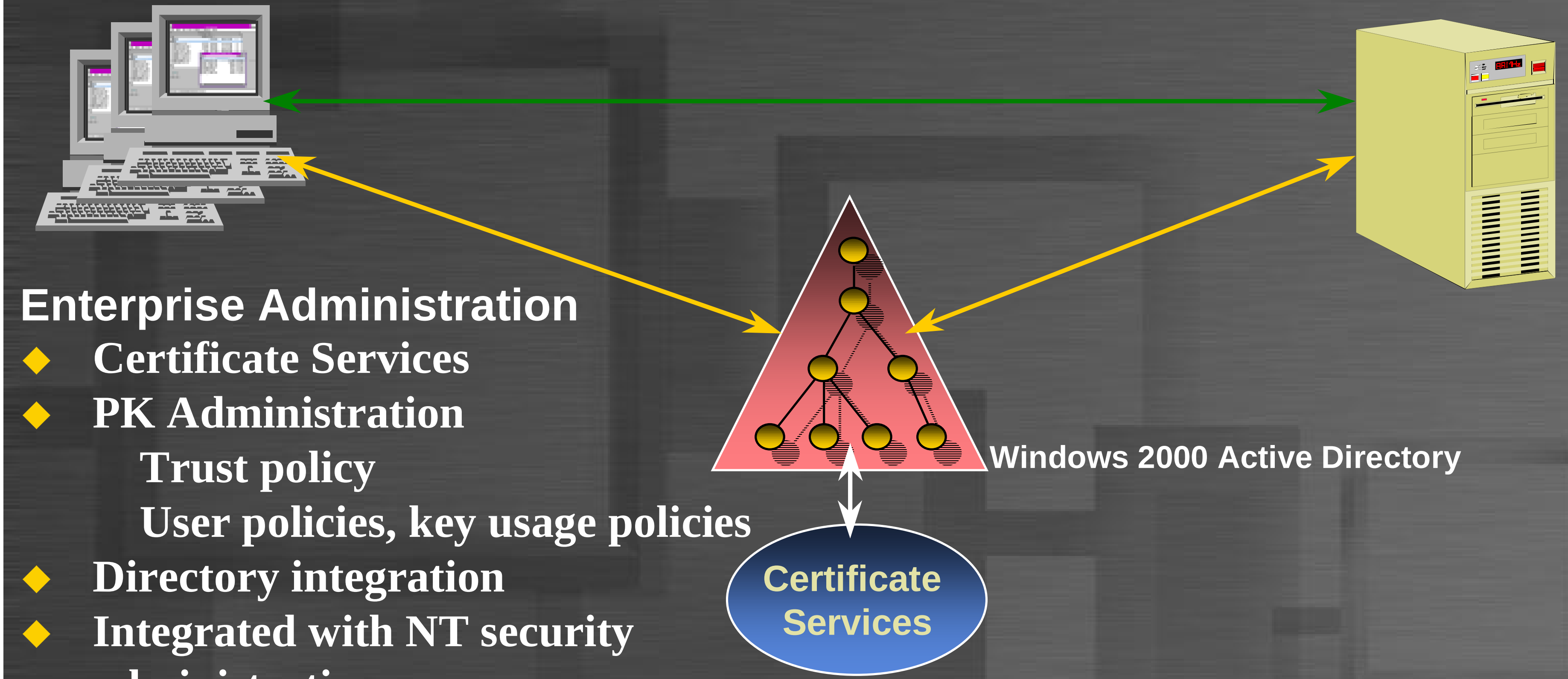
Enterprise PKI Components

Clients

- Key and certificate mgmt
- Cryptography services
- SSL/TLS
- Smart Card support

Servers

- Cryptography services
- Key and certificate mgmt
- SSL/TLS
- Client authentication



Enterprise Administration

- Certificate Services
- PK Administration
  - Trust policy
  - User policies, key usage policies
- Directory integration
- Integrated with NT security administration

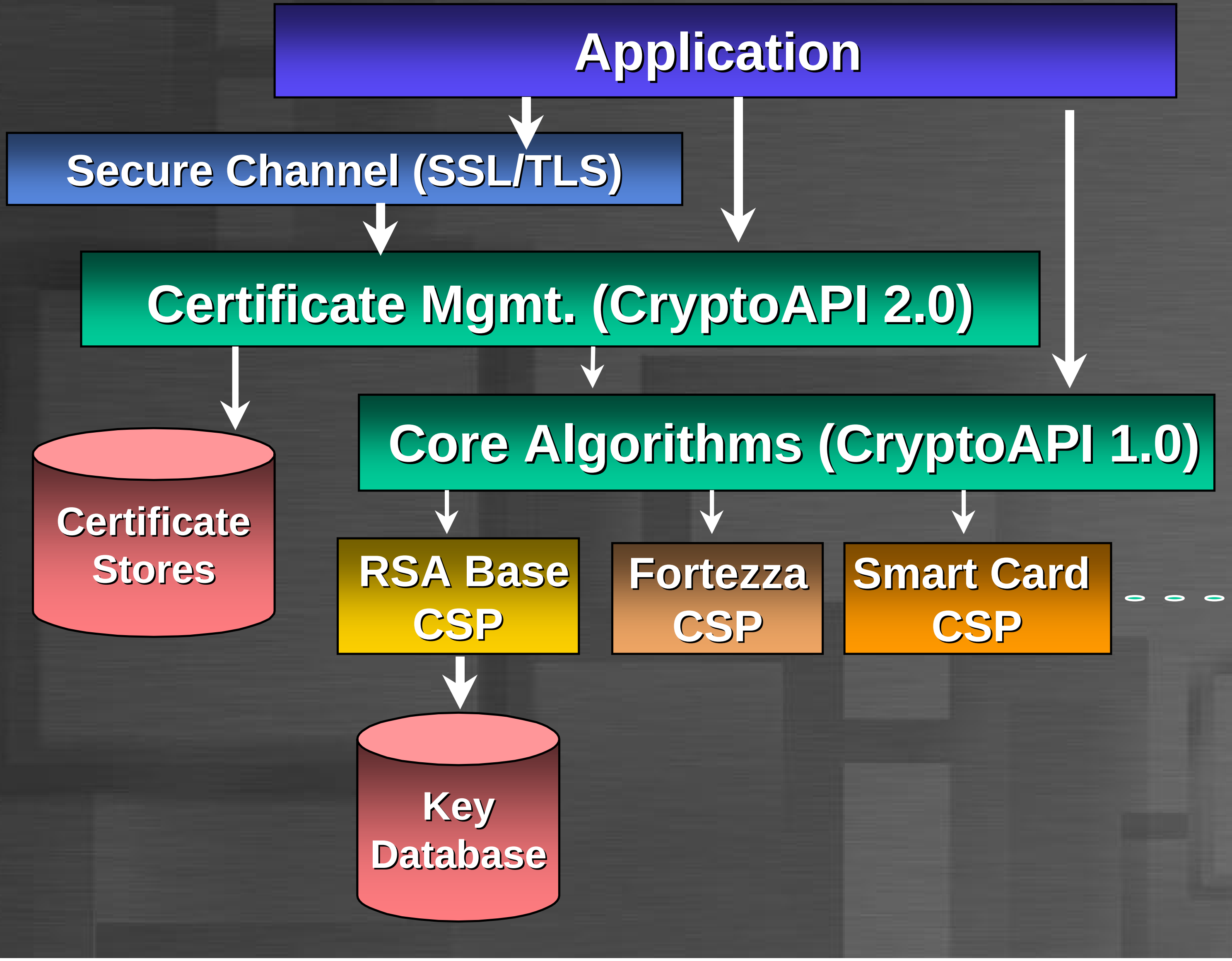
New Core Functionality in Windows 2000

- Standards support in Windows 2000
- CryptoAPI 1.0 – Algorithms
- CryptoAPI 2.0 – Certs & Messages
- SChannel (SSL/TLS)
- Smart Cards

Supported PKI Standards

- X.509/IETF-related standards
  - X.509/PKIX Part 1 certificates & CRLs
  - S/MIMEv2 (v3 in progress)
  - TLS 1.0 (follow-on to SSL3)
- PKCS-related standards
  - PKCS 10 & 7 for certificate enrollment
  - PKCS 12 for migration of key material
- FIPS 140-1 validation (in process)
- PC/SC for smart cards

CryptoAPI Framework



Application

Secure Channel (SSL/TLS)

Certificate Mgmt. (CryptoAPI 2.0)

Certificate Stores

Core Algorithms (CryptoAPI 1.0)

RSA Base CSP

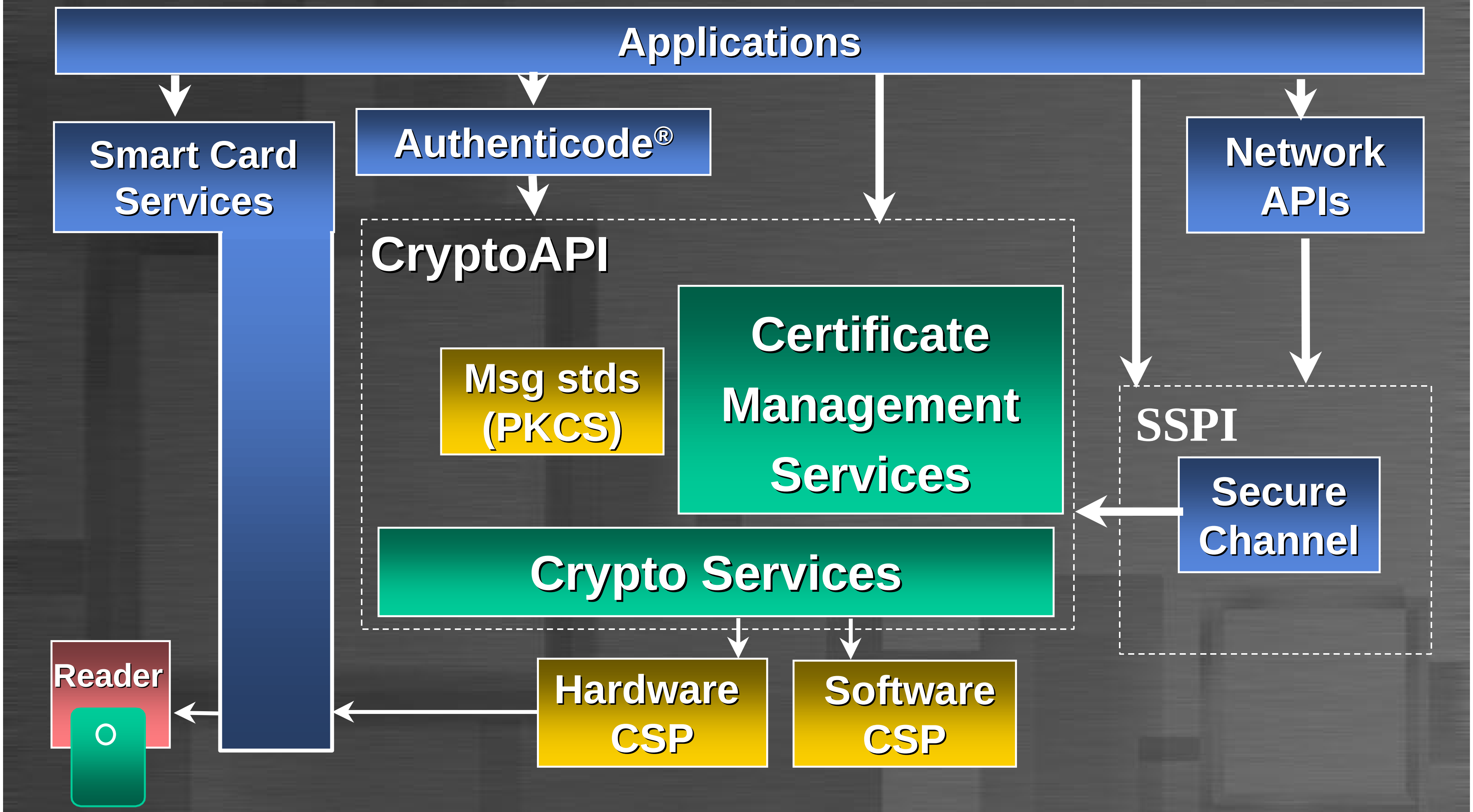
Fortezza CSP

Smart Card CSP

- - -

Key Database

Windows 2000 PK Architecture



Algorithm Enhancements

- DSS/DSA signatures
- Diffie-Hellman (as part of TLS 1.0)
- Greater security for private key material
  - Migration from Protected Storage (PStore) to Data Protection APIs (DPAPI)
  - Enhanced PKCS#12 support

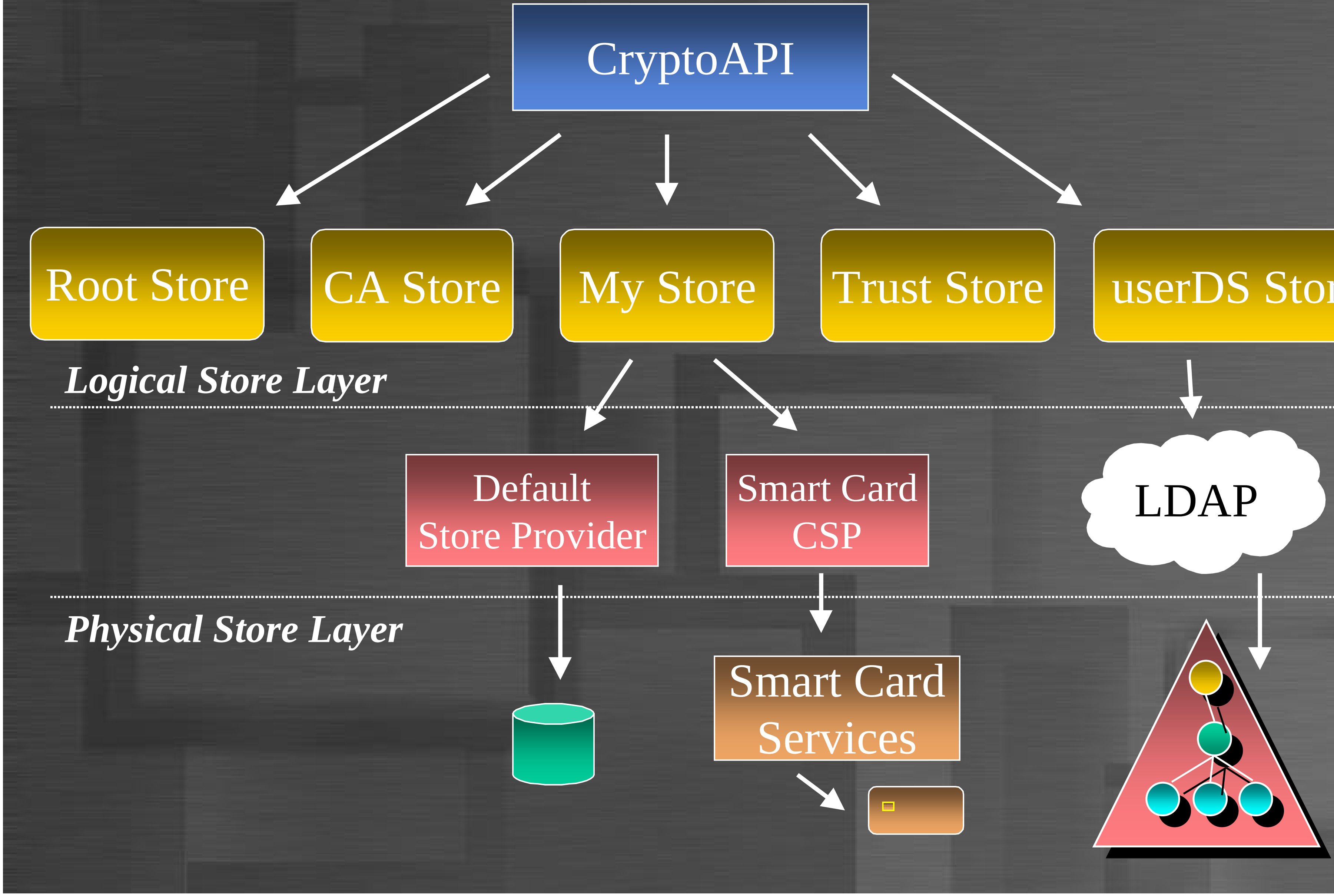
Certificate Enhancements

- Certificate store improvements
- Certificate chain building & validation
- Certificate revocation & CRLs
- Common UI components

Certificate Stores

- Plug-able provider model
- New providers in NT5
  - Logical cert stores & inheritance
  - LDAP stores
  - HTTP (generic URL) stores
- Default per-user/per-machine stores

Certificate Storage Model



CryptoAPI

Root Store

CA Store

My Store

Trust Store

userDS Store

Logical Store Layer

Default Store Provider

Smart Card CSP

LDAP

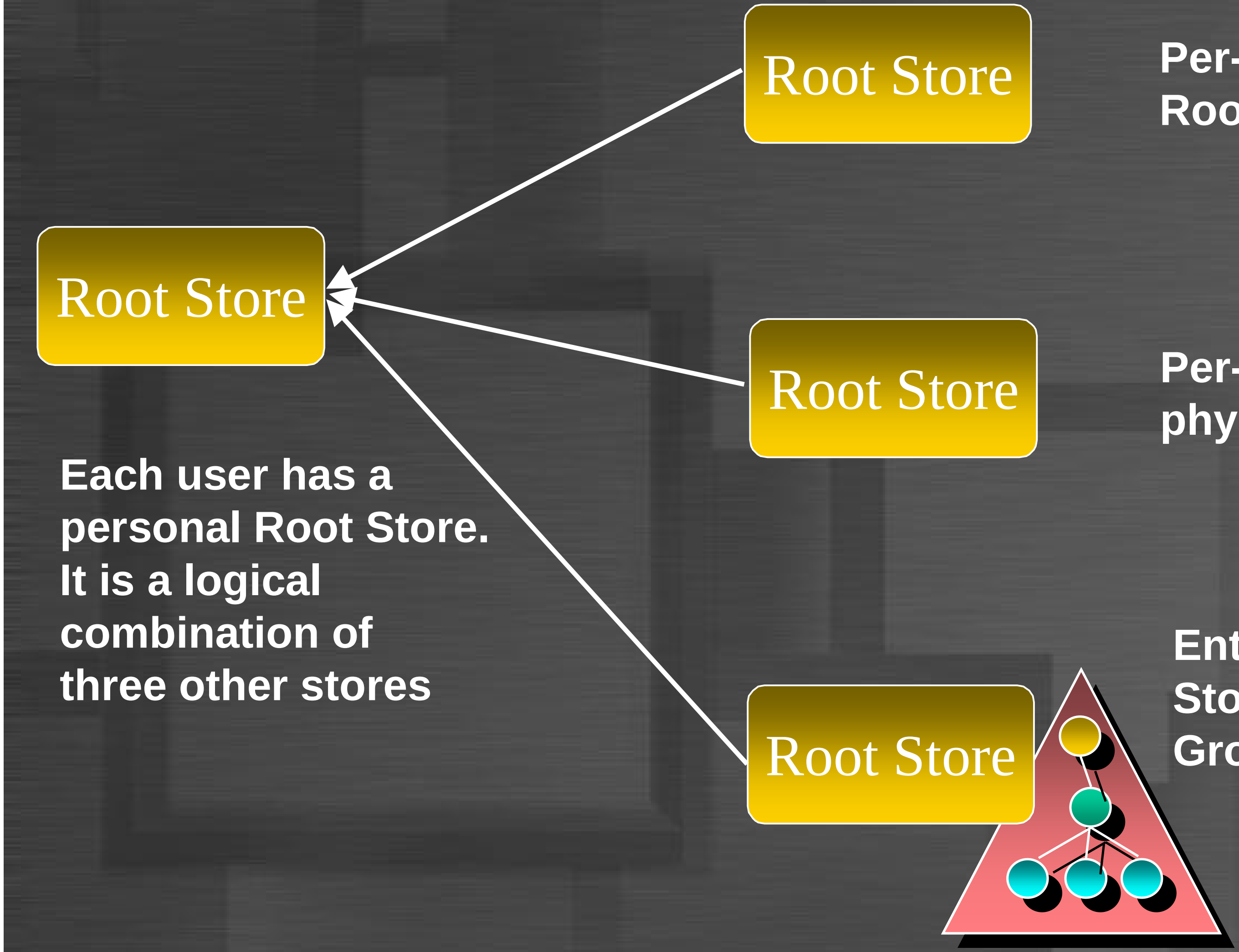
Physical Store Layer

Smart Card Services

Certificate Stores

- Trusted Root Certification Authorities
  - Self-signed, implicitly-trusted CA certificates
- Personal
  - End-entity (EE) certificates associated with personally-held private keys
- Intermediate Certification Authorities
  - Certificates for intermediate CAs and other EEs

Cert Store Inheritance



Root Store

Root Store

Per-user physical Root Store

Root Store

Per-machine physical Root Store

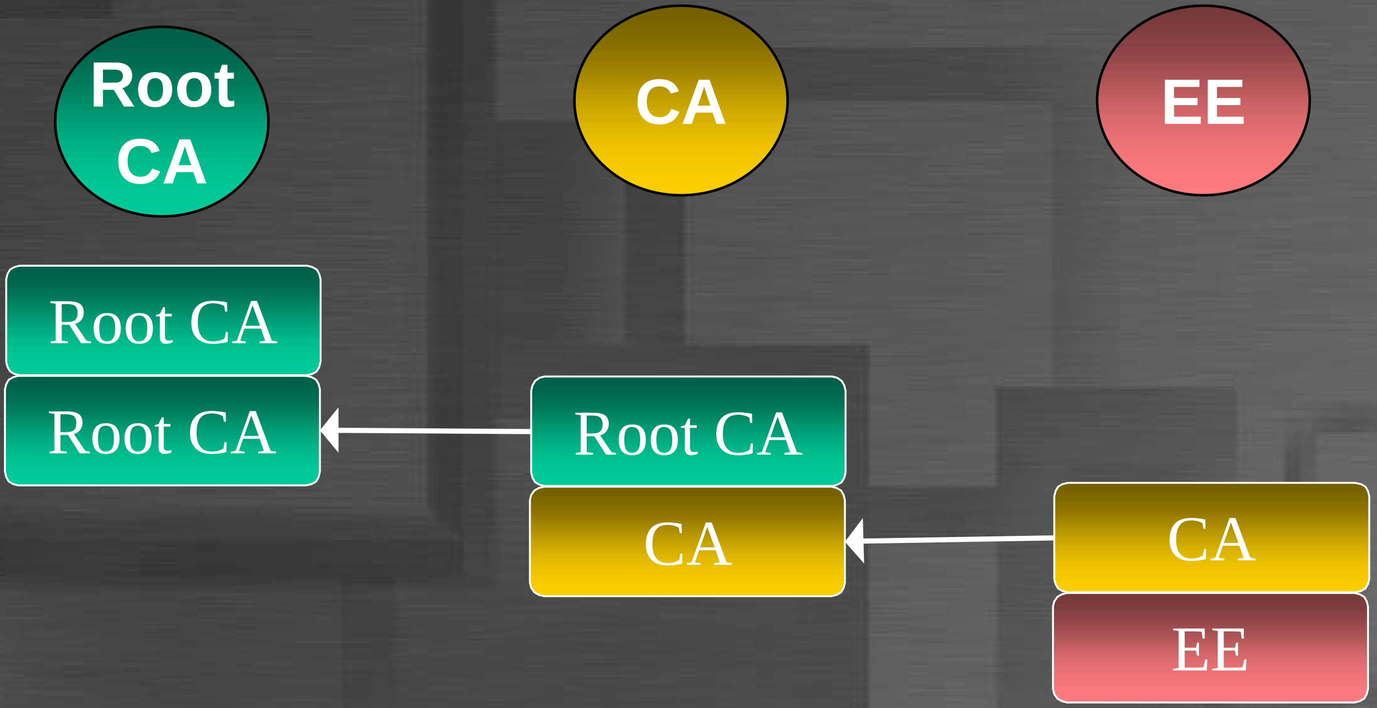
Root Store

Enterprise-wide Root Store (part of Enterprise Group Policy)

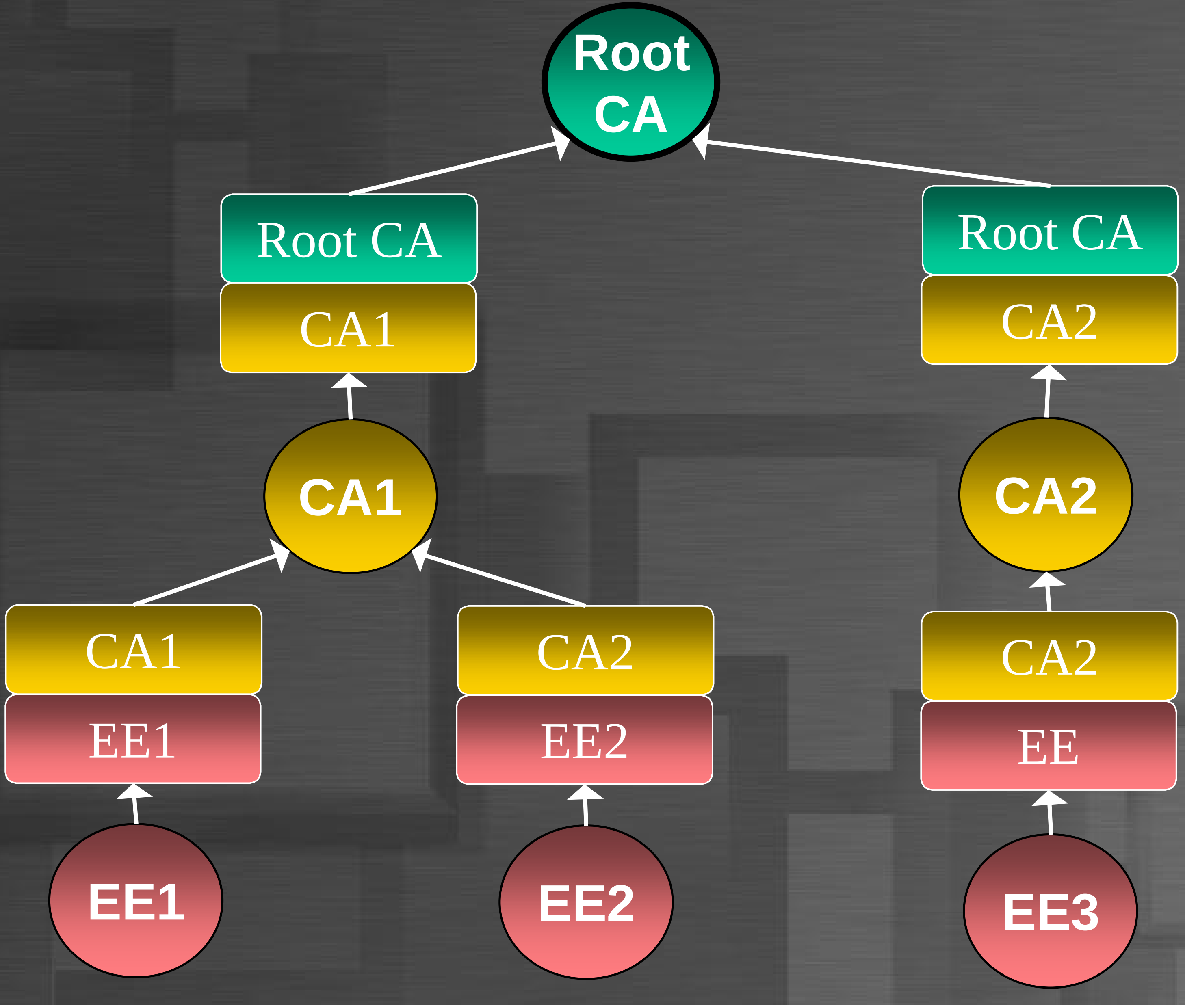
Each user has a personal Root Store. It is a logical combination of three other stores

Chain Building & Validation

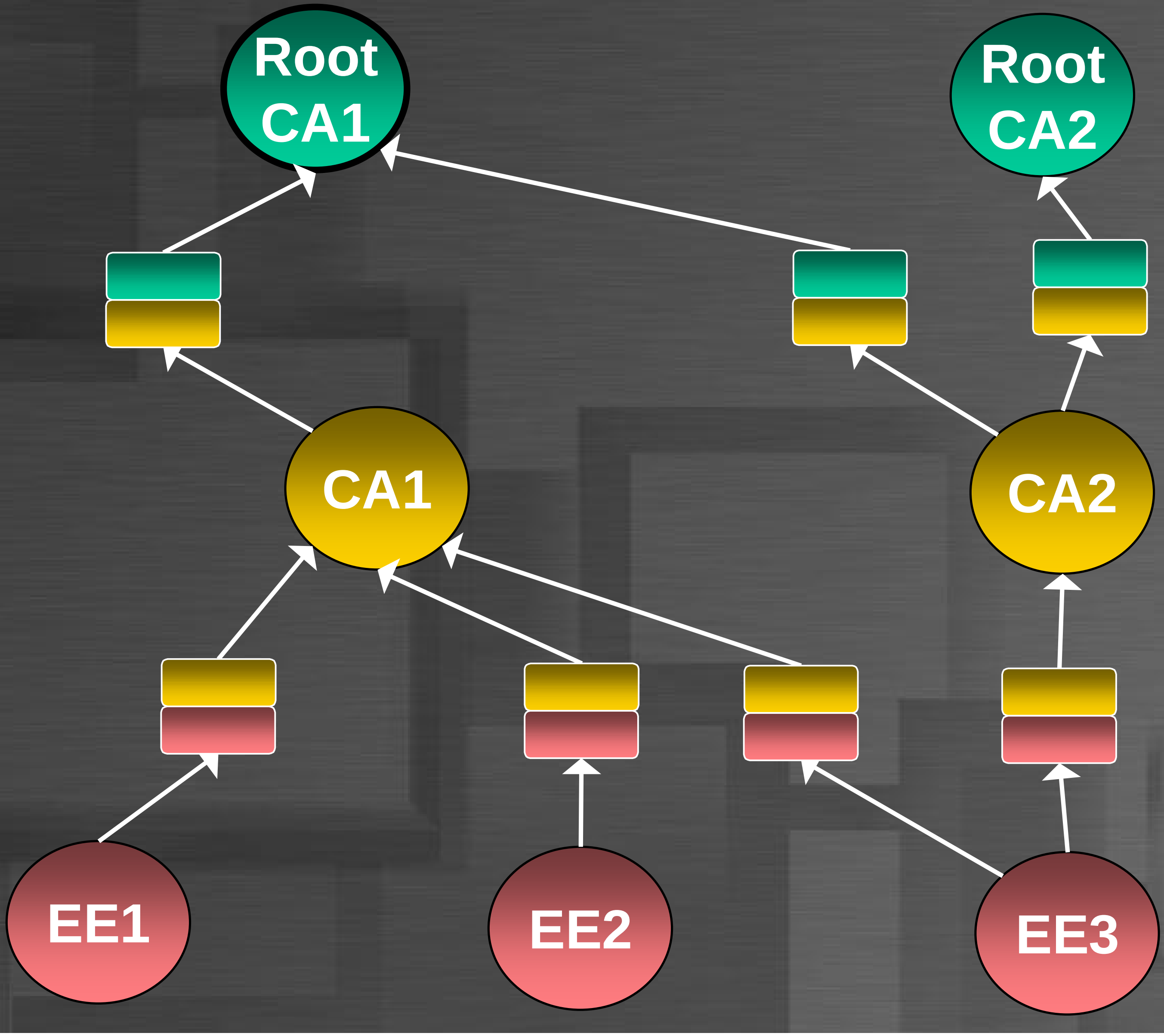
- "Given an end-entity certificate, does there exist a cryptographically valid chain of certificates linking it to a trusted root certificate?"



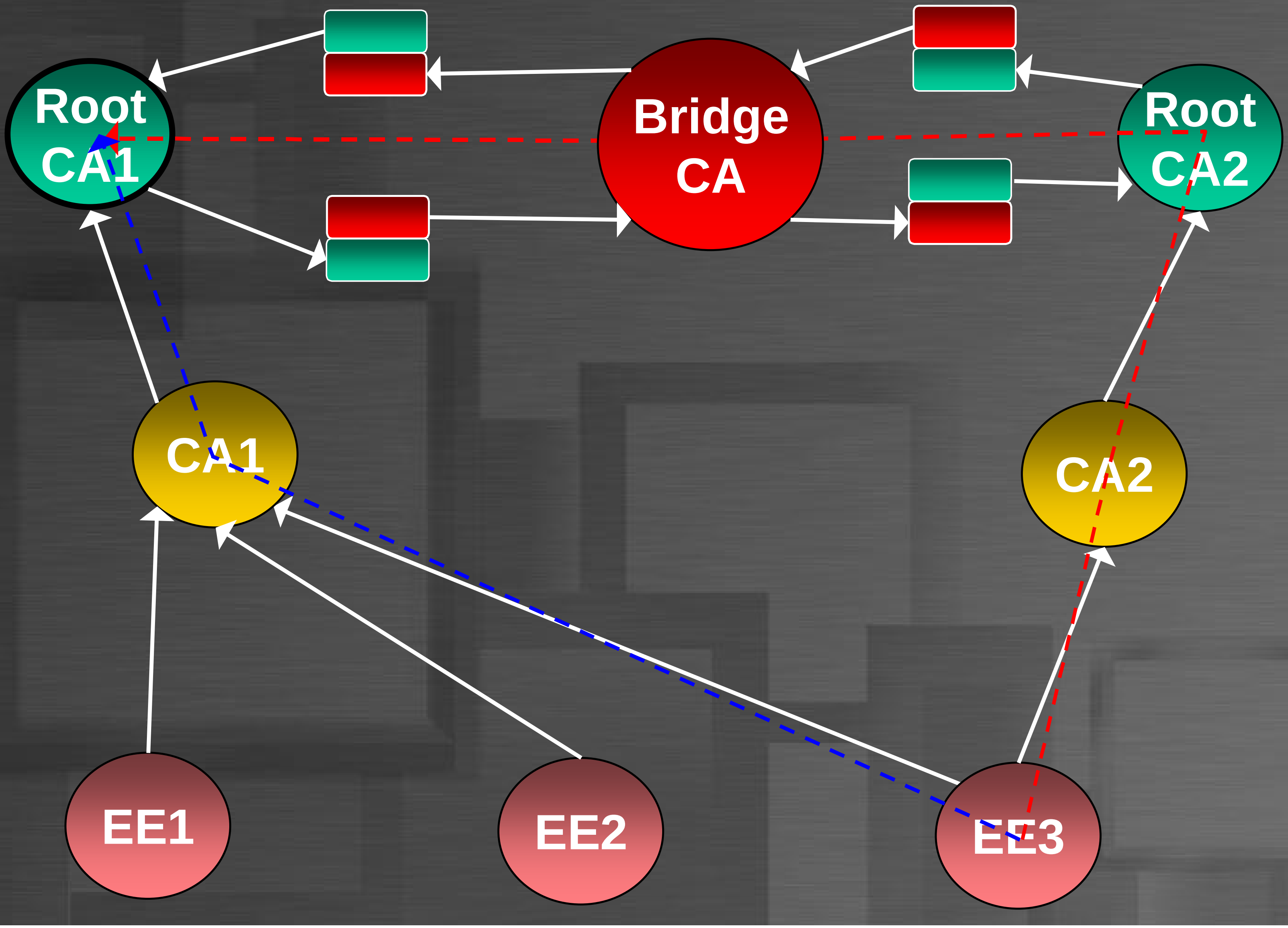
Chain Building Details (1)



Chain Building Details (2)



Chain Building Details (3)



Revocation

- CryptoAPI chain building will (optionally) perform automatic revocation checking.
  - Any CryptoAPI application (e.g. Internet Explorer, IIS, Outlook Express and Smart Card Logon) can get revocation checking “for free.”
- Relevant CRLs are located using pointers in CRL Distribution Point cert extensions
- First CRL reference retrieves CRL from one of the publication points
- Subsequent references use local cache of valid CRLs

SChannel Enhancements

- Addition of support for IETF TLS 1.0 as part of SChannel
- SChannel uses CryptoAPI 2.0 chain-building logic
- Export control-related issues:
  - Better server-gated crypto (SGC) logic to support more SGC issuers
  - 56-bit DES & 1024-bit asymmetric keys

Smart Cards

- RSA cryptographic cards supported through CryptoAPI
  - Gemplus, Schlumberger “in the box”
- WHQL reader logo program
  - Gemplus, Bull, SCM Microsystems, Litronic, Rainbow Technologies
- User roaming supported

Agenda

- Windows 2000 PKI core components
- Client-side PKI components
  - Internet Explorer 5.0
- Server-side PKI components
  - Windows 2000 Certificates Services
- Enterprise-wide PKI features
  - Administration of enterprise-wide PKI policy

Client-side PKI Components

- Common viewers for certificates, digital signatures on objects
- Wizards for enrollment, cert/key import & export, digital signing
- Two certificate management interfaces
  - Lightweight cert manager, part of IE 5.0
  - Cert manager MMC snap-in

Client-side PKI Demo

- SSL/TLS connections in IE 5.0
- Common certificate dialog/viewer
- IE 5.0 “lightweight” cert manager
- Certificate & private key import
- Enterprise certificate enrollment

Demo

Certificate Enrollment

- Request certificate for a key pair
  - Client-side, single-key
  - Online and offline
- Three methods for Users
  - Win32 Wizard
  - Web using ActiveX control
  - Enroll-on-behalf for smart card
- Computers
  - Automatic through Group Policy

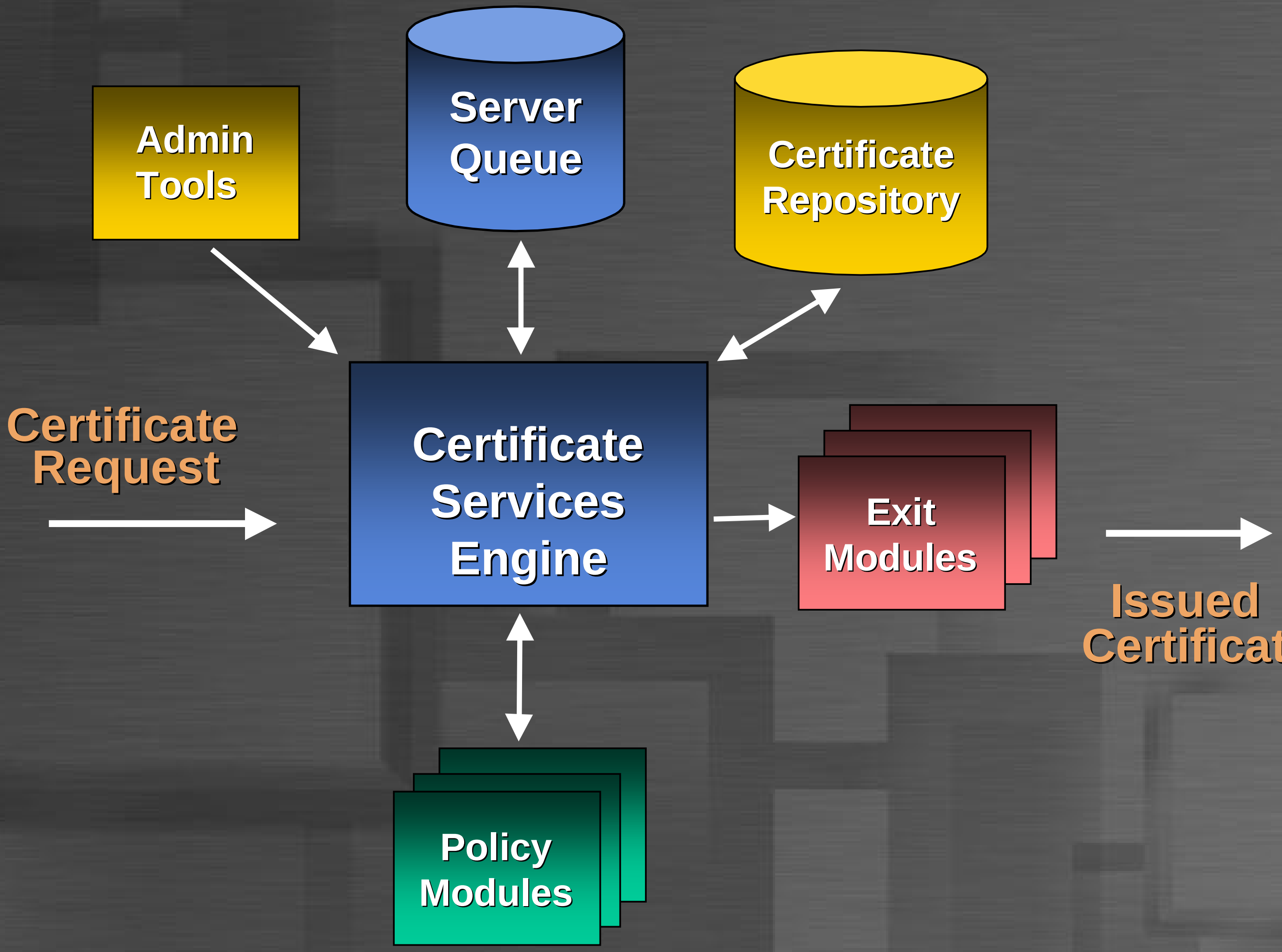
Agenda

- Windows 2000 PKI core components
- Client-side PKI components
  - Internet Explorer 5.0
- Server-side PKI components
  - Windows 2000 Certificates Services
- Enterprise-wide PKI features
  - Administration of enterprise-wide PKI policy

Certificate Services

- Scalability
- Enterprise Policy
  - Integration with the Active Directory for publication of certs & CRLs
- Certificate types/templates
  - Standard types of issued certs (e.g. “User” or “Smart Card Logon”)
  - Stored & ACL’d in the Active Directory
- CRL publication

Certificate Services Architecture



Admin Tools

Server Queue

Certificate Repository

Certificate Request

Certificate Services Engine

Exit Modules

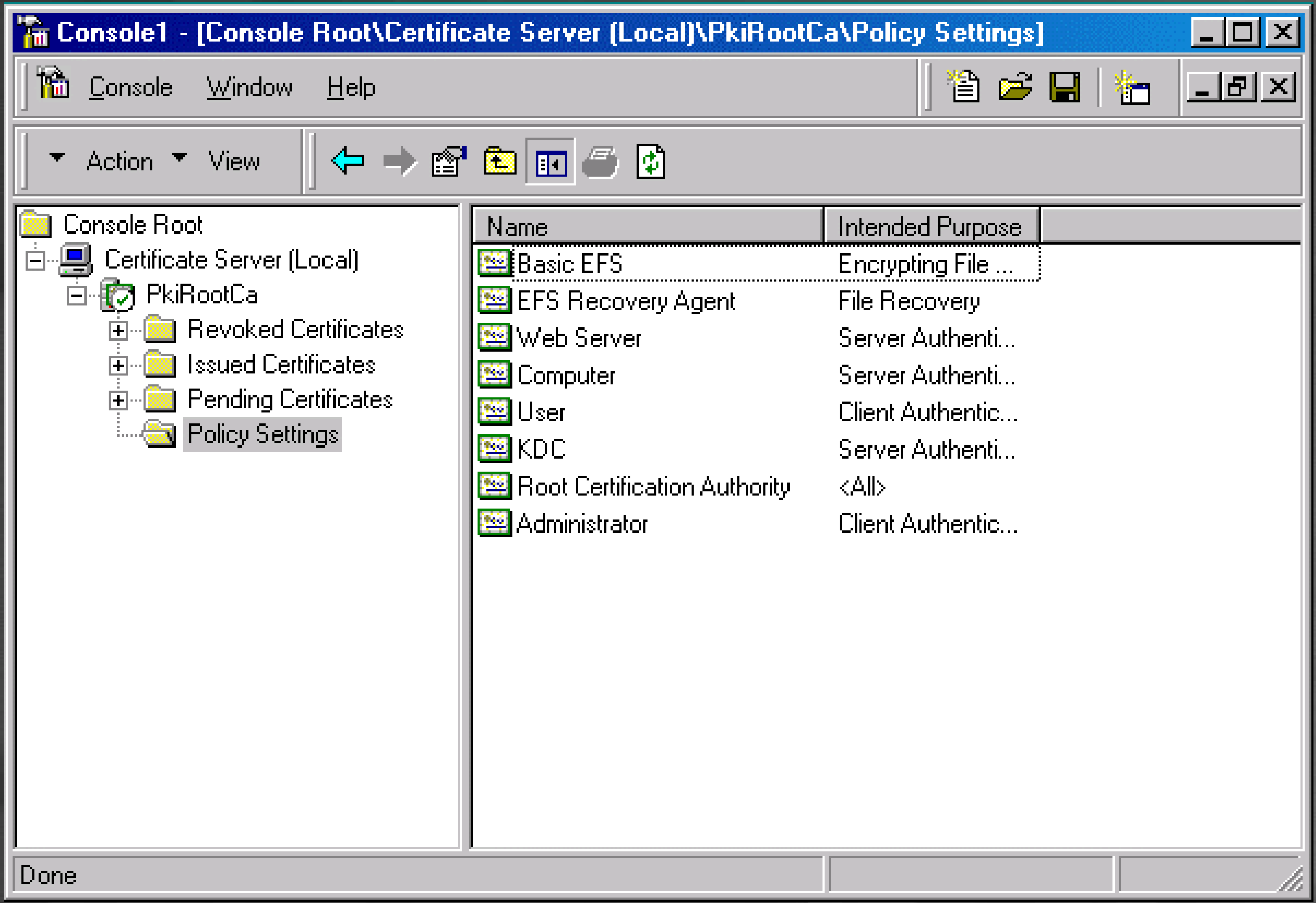
Issued Certificate

Policy Modules

Types of CAs

- Enterprise
  - Authenticates requests via NT accounts
  - CA object published in Active Directory
- Standalone
  - Does not authenticate via NT accounts
- Exchange
  - KMS-specific policy module
  - KMS provides key archival/recovery for email

Certificate Services Manager



Name	Intended Purpose
Basic EFS	Encrypting File ...
EFS Recovery Agent	File Recovery
Web Server	Server Authenti...
Computer	Server Authenti...
User	Client Authentic...
KDC	Server Authenti...
Root Certification Authority	<All>
Administrator	Client Authentic...

Certificate Revocation Lists

- Revoke certificates using Certificate Services Manager
- Publish revocation lists
  - Automatic intervals (daily, weekly)
  - Manual
- CRLs published to multiple access points
  - Active Directory (LDAP)
  - CA server (HTTP, SMB)

Agenda

- Windows 2000 PKI core components
- Client-side PKI components
  - Internet Explorer 5.0
- Server-side PKI components
  - Windows 2000 Certificates Services
- ➢ Enterprise-wide PKI features
  - Administration of enterprise-wide PKI policy

Enterprise PKI Admin and Policy

- “Who controls PKI trust policies?”
- PKI Integration with the Active Directory
- Manage public key policy settings via the Group Policy Editor
  - Domain trusted root authorities
  - Certificate issuance policy

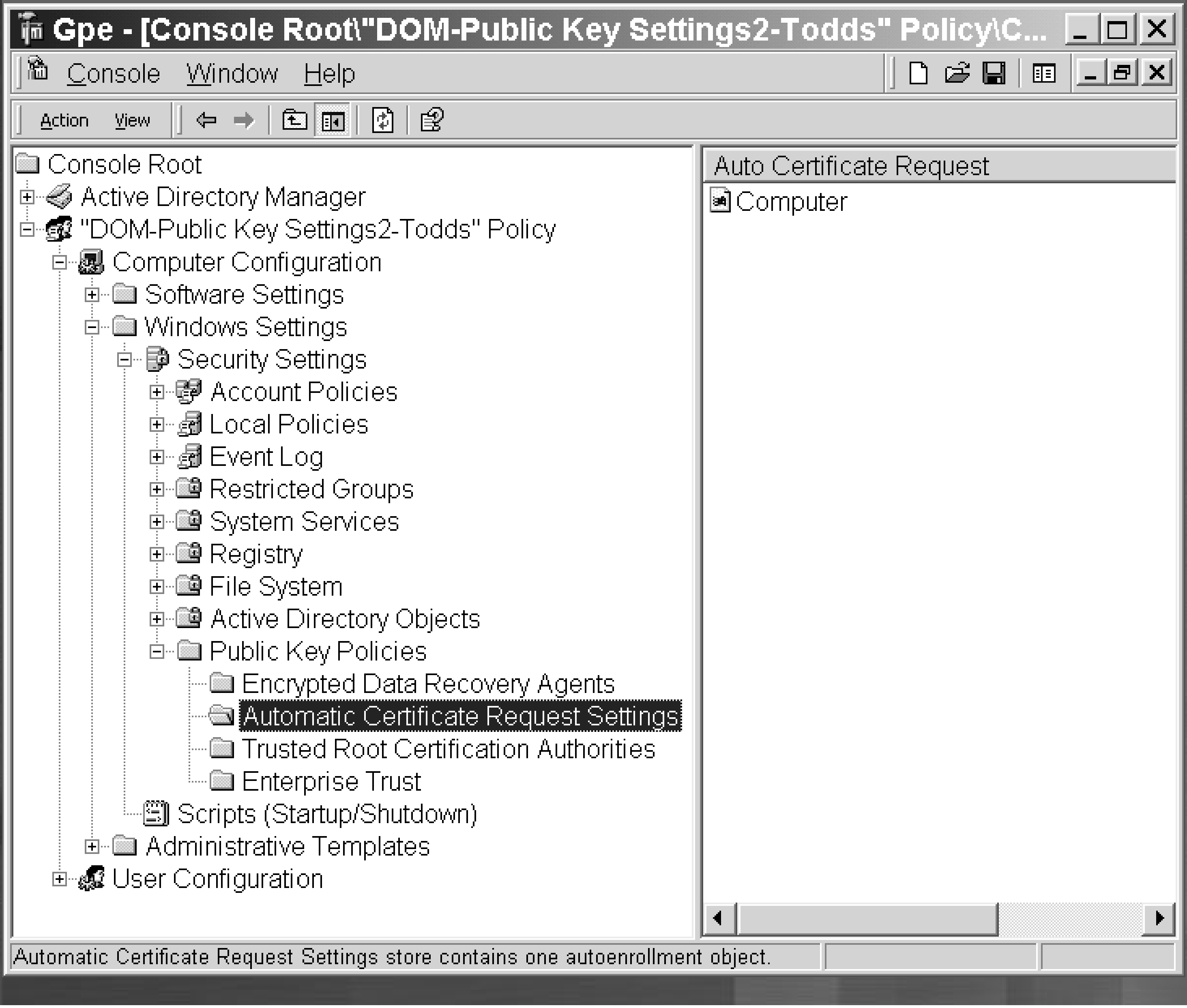
PKI Integration with the Active Directory

- Automatic publication & retrieval of PKI objects
  - Certificates
  - Per-CA CRLs
- Automatic certificate mapping to users & machines in the directory
- Policy administration & propagation

Public Key Policy Settings

- Trusted Root Certification Authorities
  - Sources of implicit trust
- Certificate Templates (ACLs)
- Certificate Trust Lists
  - Constrain external roots by purpose
- Automatic Certificate Enrollment
  - For machine certificates

Group Policy Editor



Gpe - [Console Root\"DOM-Public Key Settings2-Todds" Policy\C...
Console
Window
Help
Action
View

- Console Root
  - Active Directory Manager
  - "DOM-Public Key Settings2-Todds" Policy
    - Computer Configuration
      - Software Settings
      - Windows Settings
        - Security Settings
          - Account Policies
          - Local Policies
          - Event Log
          - Restricted Groups
          - System Services
          - Registry
          - File System
          - Active Directory Objects
          - Public Key Policies
            - Encrypted Data Recovery Agents
            - Automatic Certificate Request Settings
            - Trusted Root Certification Authorities
            - Enterprise Trust
        - Scripts (Startup/Shutdown)
      - Administrative Templates
    - User Configuration

Auto Certificate Request

Computer

Automatic Certificate Request Settings store contains one autoenrollment object.

Leveraging Windows 2000 PKI in Applications

- S/MIME encryption & digital signatures (OL98/2000, OE5)
- SSL/TLS
  - Server authentication (IIS5)
  - Client authentication (IE5)
- IPSec (in cert-based mode)
- Encrypting File System (EFS)
- Smart-card logon (PKI & Kerberos)

Summary

- PKI is a core component of the Windows 2000 platform
  - Client-side/core services (CryptoAPI, SChannel)
  - Certificate Services on Windows 2000 Server
  - Enterprise-wide administration of PKI trust policies
  - PK-aware applications (S/MIME, IPSec)